DISCUSSION OF PUBLIC COMMENTS RECEIVED

ON THE AUTOMATED TARGETING SYSTEM

SYSTEM OF RECORDS NOTICE

PUBLISHED NOVEMBER 2, 2006 (71 FR 64543)

On November 2, 2006, Customs and Border Protection (CBP), an agency within the Department of Homeland Security (DHS), issued a system of records notice (SORN) under the Privacy Act (5 U.S.C. 552a) for the Automated Targeting System (ATS) (71 FR 64543). DHS received a number of comments and decided to extend the comment period until December 29, 2006, by Federal Register Notice dated December 8, 2006 (71 FR 71182). A total of 641 comments were received in response to the SORN. The following is an analysis of the comments and questions submitted by the public.

General Comments

Comment: CBP must consider all available information when conducting customs examinations at the border.

Response: DHS concurs. The availability of advance electronic information is crucial for CBP to prevent potentially high-risk persons, conveyances and shipments from entering the United States while maintaining the flow of lawful travel and trade. The 9/11 Commission recommendations, the Intelligence Reform and Terrorism Protection Act (IRTPA), and CBP's experiences all point towards the use of advance information in automated systems to intercept terrorist suspects and shipments of

weapons of mass effect, as well as to identify other violations of U.S. law with respect to persons, conveyances and cargo seeking to cross the U.S. border.

Comment: Most elements of Passenger Name Records (PNR) do not satisfy the criterion for protection under the Privacy Act.

Response: CBP collects PNR data pursuant to 19 CFR 122.49d. This information is stored by the Automated Targeting System (ATS) in its passenger module, ATS-P. PNR is comprised wholly of data that certain air carriers collect as part of their usual business practice of negotiating and arranging travel transactions. Thus, PNR contains personally identifiable information (PII) that, at a minimum, includes the name of the person traveling and the person who submitted the information as part of arranging the travel, to include travel professionals, who make reservations for a passenger, operator or crew member. The Privacy Act requires that CBP create a SORN for any system of records (as defined at 5 U.S.C. 552a(a)(5)) that it maintains. Once CBP has created a SORN to inform the public of its collection and the practices employed to protect certain data, it applies the same rules and protections to all information maintained within the system, including information on individuals other than U.S. citizens and Lawful Permanent Residents (LPR) (*see* http://www.dhs/xlibrary/assets/privacy_policyguide_2007-1.pdf). Individuals, regardless of nationality, may seek access to records about themselves in accordance with the Freedom of Information Act (FOIA). In addition, as a matter of administrative policy, DHS has adopted the practice of handling non-U.S. individuals' PII that is held in mixed systems in accordance with the fair information principles set forth in the Privacy Act.

Under this policy, DHS does not distinguish between U.S. Citizens, LPRs, or foreign nationals with regard to storage, sharing and access to PNR data collected in ATS-P.

Absent an exemption under the Privacy Act, non-U.S. individuals are able to access their PII and amend their records; however, this administrative policy does not extend or create any cause of action or right of judicial review for non-U.S. individuals. This administrative policy cannot provide remedies under the Privacy Act that exceed DHS's administrative discretion.

Comment: Traveler profiling based on relevant facts is legal and effective.

Response: Travelers that ATS—and more specifically, ATS-P—identifies for possible further scrutiny are not selected because of any objective physical characteristic or political, religious, racial, or ethnic affiliation. Travelers are so identified as the result of threshold targeting rules in ATS, which are based on current intelligence or past case experience. Travelers may also be identified for further screening if their date of birth or identifier match an entry placed for subject query in the Treasury Enforcement Communications System (TECS). A subject query is a query of records that pertains to persons, aircraft, businesses, or vehicles.

Comment: DHS needs to establish that the system works.

Response: This comment reflects a common misconception regarding ATS—i.e., that the information technology comprising ATS is in its infancy. ATS-P has been operational under the TECS SORN since approximately 2000, and the cargo components of ATS have been operational since approximately 1997. The purpose of this notice is to remove ATS from coverage under the TECS SORN and create a separate SORN for ATS

to provide the public with increased notice and transparency regarding CBP's screening efforts.

Comment: ATS represents an unprecedented increase in surveillance by CBP.

Response: Throughout its 218 year history, and beginning with actions by the First Congress of the United States, CBP and its principal legacy components, the Immigration and Naturalization Service (INS) and the U.S. Customs Service, have possessed the authority to stop and search all persons, conveyances and cargo attempting to cross the U.S. border, examine travel documents at the border, and make seizures and arrests for violations of U.S. law. ATS is merely an automated means of evaluating information in advance of arrival or departure. This advanced information and analysis allows CBP to expedite its determinations concerning potentially high-risk travelers, cargo, and conveyances that require further inspection.

Comment: Mission creep is built into ATS.

Response: ATS is designed to assist CBP in enforcing customs and immigration laws as well as the myriad other U.S. laws CBP is responsible for enforcing at the border. Indeed, in addition to enforcing the customs (Title 19) and immigration laws (Title 8) of the U.S. Code, as the pre-eminent presence at the nation's border CBP is also required to step into the shoes of numerous other federal agencies and, at their behest, ensure compliance with laws and regulations covering a wide spectrum of subjects, including: the Agricultural Bioterrorism Protection Act of 2002 (7 USC § 8401); the Honeybee Act (7 USC § 281-286); the Export Administration Act of 1979 (15 USC § 4605); the Copyright Act (17 USC § 101-120); the Clean Air Act (42 USC § 7521-7543); and the Trading with the Enemy Act (50 USC App § 1-44). While ATS can be re-designed to

rapidly respond to changes in the law and changes in intelligence to maximize the law enforcement capabilities of CBP officers, a number of administrative and policy checks and balances exist to ensure that the use of ATS remains within the appropriate bounds of the mission of DHS. For example, CBP uses the PNR stored in ATS-P in a well-defined fashion—namely, (1) to prevent and combat terrorism and related crimes: (2) to prevent and combat other serious crimes, including organized crime, that are transnational in nature; (3) to prevent flight from warrants or custody for crimes described above; (4) wherever necessary for the protection of the vital interests of a data subject or other persons; (5) in any criminal judicial proceedings; or (6) as otherwise required by law.

Comment: The deployment of ATS will have a detrimental economic impact.

Response: As noted before, the cargo modules of ATS as well as ATS-P have been deployed since approximately 1997 and 1999, respectively. In that time, no detrimental impact to trade or travel has occurred. To the contrary, ATS has facilitated the processing of legitimate trade and travel by allowing advanced screening to help direct CBP's enforcement efforts to those persons and property which require further scrutiny by officials. The purpose of the SORN is to provide greater notice and transparency with respect to these screening activities. ATS is a decision-support tool that assists CBP in more effectively discharging its inspectional duties.

Access and Redress Comments

Comment: The ATS SORN allows CBP to use the risk assessment ATS generates for a wide variety of purposes and does not provide individuals with the ability to seek redress to correct underlying personal information that is inaccurate.

Response: CBP agrees that administrative access to the PNR data by the subject of the information under the Privacy Act should be permitted. CBP published a revised SORN for ATS on August 6, 2007 which amends the ATS SORN issued in November 2006 to clarify that existing policy allows persons (including foreign nationals) to seek access under the Privacy Act to the PNR submitted to ATS-P. With respect to the ATS-P module, no exemption from access provisions of the Privacy Act are asserted regarding PNR about the requester which is obtained from a booking agent, brokers, or another person on the requester's behalf, or the requester himself. This information, upon request, may be provided to the requester in the form in which it was collected from the respective carrier, but may not include certain business confidential information of the air carrier that is also contained in the record. For the other ATS modules (cargo, conveyance, etc.), the only information maintained in ATS is the risk assessment analyses and pointers to information within other sources of records.

In addition to the SORN, DHS has also published a Notice of Proposed Rulemaking which identifies the exemptions to the certain provisions of the Privacy Act claimed for ATS, including ATS-P, and explains the reasons for the exemptions claimed for these records.

With regard to the matter of redress, CBP also notes that ATS is a decision-support tool that compares various databases, but does not actively collect the information from those respective databases. The one exception to this process is PNR, which is collected for ATS-P. When an individual is seeking redress for other information analyzed in ATS, such redress is properly accomplished by referring to the databases that directly collect that information.

To facilitate the redress process, DHS has created a comprehensive, Government-wide program, the Traveler Redress Inquiry Program (TRIP) (*see,* 72 Fed. Reg. 2294, January 18, 2007), to receive all traveler related comments, complaints, and redress requests affecting its component agencies. Through TRIP, a traveler can seek correction of erroneous PNR information stored in ATS and information stored in other DHS databases.

Inaccurate Information Comments

Comment: There is a high likelihood of false positives and inaccurate bad information.

Response: ATS-P's use of information, including PNR data and information from the Advance Passenger Information System (APIS), actually decreases the risk of traveler misidentification because it allows officers to review and resolve possible concerns prior to the traveler's arrival. Without ATS-P, all concerns would have to be reviewed and resolved upon the traveler's arrival at the port of entry, which would create significant delays.

Comment: CBP should be civilly and criminally liable for the negative consequences or the incorrect actions taken against travelers as a result of inaccurate information contained in ATS-P.

Response: ATS-P is a decision-support tool that assists CBP Officers in identifying individuals who warrant additional screening—which ranges from clarifying a missing middle initial to referral to secondary examination. Any legal actions against travelers, from seizures of contraband to felony arrests to denials of admissibility, are the

result of a CBP officer's hands-on interaction and examination of a person and consideration of additional evidence or information obtained from other sources. Importantly, ATS-P does not by itself result in final administrative or criminal actions against travelers.

Comment: CBP lacks competence to maintain or understand PNR.

Response: CBP (and legacy U.S. Customs Service) has used PNR to perform advanced screening of travelers since the early 1990s. Starting in 1999, legacy U.S. Customs Service received this information electronically from certain air carriers on a voluntary basis, and in 2002 this was mandated from all commercial air carriers pursuant to ATSA. CBP officers, and those of legacy U.S. Customs Service and U.S. Immigration and Naturalization Service, have successfully used and interpreted PNR data to intercept hundreds of terrorist suspects and criminal violators, to prevent countless incidents of contraband smuggling, and to identify a constant stream of human smugglers. All along, CBP and its legacy agencies have effectively safeguarded and secured PNR.

40 year Retention Period Comments

Comment: The 40 year retention described in the ATS SORN is too long and too expensive.

Response: Terrorist suspects often have no prior criminal record and, at the time of travel, the U.S. Government may have no other derogatory background information about them. CBP uses PNR, including historical PNR, to attempt to identify such previously unknown travelers before they enter the United States. Specifically, ATS-P is able to

analyze PNR data to uncover links between known and previously unidentified terrorists or terrorist suspects, as well as suspicious or irregular travel patterns.

CBP has determined that it can continue to uncover this information with a shorter retention period. CBP believes that this decision will also enhance privacy protections for travelers whose information is collected. The retention period for information maintained in ATS will not exceed fifteen years, after which time it will be deleted in accordance with an approved records disposition schedule except as noted below.

Additionally, the following further access restrictions pertain to the retention and use of PNR, which is contained only in ATS-P: ATS-P users will have general access to PNR for seven years, after which time the PNR data will be moved to dormant, non-operational status. PNR data in dormant status will be retained for eight years and may be accessed only with approval of a senior DHS official designated by the Secretary of Homeland Security and only in response to an identifiable case, threat, or risk.

Notwithstanding the above, information that is maintained only in ATS that is linked to law enforcement lookout records, CBP matches to enforcement activities, investigations or cases (*i.e.*, specific and credible threats, and flights, individuals and routes of concern, or other defined sets of circumstances)—will remain accessible for the life of the law enforcement matter.

Comment: The PNR data in storage is not secure and is subject to misuse.

Response: Multiple security measures are in place for information that is actively used by DHS for screening (referred to as production data). Although production information is not encrypted, CBP uses routers, firewalls, and intrusion detection systems to prevent unauthorized access to its systems. Any information stored via backup tape is

protected through strict physical and other technical safeguards to ensure it cannot be inappropriately accessed.

Sharing Comments

Comment: Third parties are given inappropriate access and/or the sharing is too extensive.

Response: CBP, and its predecessor agencies the U.S. Customs Service and the Immigration and Naturalization Service, have signed MOUs or entered into agreements with a wide variety of federal, state, and local agencies with an interest in maintaining border security and law enforcement; similar accords are in place with other nations in the form of customs mutual assistance agreements (CMAAs). The terms of these MOUs or agreements specify the necessity of sharing information and highlight the fact that the types of information sharing described in the SORN are neither unique nor recent in nature for border authorities. Additionally, all MOUs and agreements for the sharing of information contain specific provisions relating to the responsibilities of the receiving party to keep the information confidential, protected, and secure. DHS does not share PII with domestic or foreign governments or multilateral organizations which DHS is not confident will protect the privacy interests of the data subject.

The routine uses identified are consistent with CBP's role as a law enforcement agency that enforces over 400 statutes on behalf of more than 40 agencies in the Federal Government. DHS is charged in its authorizing statute, specifically section 892 of the Homeland Security Act of 2002, to facilitate the sharing of terrorist information across the government. In addition, The Intelligence Reform and Terrorism Prevention Act of

2004 required the President to establish an Information Sharing Environment "that facilitates the sharing of terrorism information." Following this enactment, on October 25, 2005, the President issued Executive Order 13388, directing that DHS and other agencies "promptly give access to . . . terrorism information to the head of each other agency that has counterterrorism functions" and establishing a mechanism for implementing the Information Sharing Environment. While CBP has broad authority to share information with other government authorities, Congress specifically endorsed the sharing of PNR data with other federal agencies, particularly for national security purposes. See 49 U.S.C. 44909(c). Furthermore, all access to information through ATS is strictly governed by internal controls. With regard to ATS-P, access to PNR information and matching results is permitted through the receipt of direct requests and authorized releases, as discussed in section 5.1 of the PIA (November 24, 2006).

Privacy Act Statutory Comments

Comment: CBP should not have used the TECS SORN to cover ATS-P.

Response: The TECS SORN applies to the collection and storage of information pertaining to persons traveling across U.S. borders. ATS-P collects and maintains PNR data transmitted in advance of a person crossing the U.S. border. Because the PNR data, targeting rules, and screening results pertain to persons crossing the U.S. border or evincing the intent to do so, the collection of this information was appropriately within the scope of the TECS SORN.

Comment: ATS-P violates the "relevant and necessary" requirement of the Privacy Act.

Response: The Privacy Act requires that an agency "maintain in its records only such information about an individual as is relevant and necessary to accomplish a purpose of the agency required to be accomplished by statute or executive order of the President." 5 U.S.C. § 552a (e)(1). CBP, in consideration of its law enforcement mission, claims an exemption from this requirement. The purpose of this Privacy Act exemption is to strike a balance between protecting information collected about persons, while permitting law enforcement agencies to effectively carry out their missions. Here, the information used by ATS-P, including PNR, has a long history of supporting successful targeting and investigations and is not available from other sources to support the prescreening of travelers prior to arrival in and departure from the United States. ATS-P is a unique tool that adds to an officer's ability to identify suspicious travel. Without ATS-P, DHS would be unable to identify many travelers whose suspicious behavior is revealed only after considering past case experience and available intelligence. PNR, for example, is often only relevant when considered in light of information obtained from other law enforcement or intelligence sources. In this way, ATS-P complements and does not duplicate other border enforcement tools, such as training to identify false documents and in questioning travelers.

Comment: The ATS SORN should have disclosed fully the existence and attributes of the underlying systems that will be used by ATS.

Response: Pursuant to section 208 of the E-Government Act of 2002 and section 222 of the Homeland Security Act of 2002, notice of the various systems with which ATS interacts is provided in a Privacy Impact Assessment (PIA) in detail and generally in the SORN. Information from the underlying systems is not maintained in ATS. Only

the PNR and the risk assessment are maintained in ATS. The information from other systems of records remains in those systems; ATS queries the information in those underlying systems.

In conjunction with the revised SORN published in the Federal Register on August 6, 2007, DHS has also posted on its web site a revised PIA which discusses the various systems from which ATS regularly derives data.

Comment: The description of CBP's authority to conduct risk assessment screening in the ATS SORN is vague; the SORN does not describe how CBP handles high-risk U.S. citizens—a category of travelers that CBP cannot legally prevent from entering the United States.

Response: As described elsewhere in this document, CBP has broad constitutional and statutory authority to obtain any information from persons attempting to cross the U.S. border—including U.S. citizens—that is relevant to the enforcement of U.S. laws, including those pertaining to immigration, customs, agriculture, and myriad other laws enforced on behalf of over 40 other U.S. agencies. The various components of ATS simply automate the review of this information. Although CBP generally does not have the authority to prevent the entry of U.S. citizens into the United States, it has the authority to conduct border searches of any person seeking to cross the border to ensure compliance with U.S. laws. In the event of non- compliance, appropriate enforcement action (to include the issuance of penalties or even arrest) may be taken against a violator, including U.S. citizens.

Comment: The ATS SORN is vague, overly broad and thus violates due process because it does not define "terrorist organization," "targeting," or the consequences of targeting.

Response: The purpose of a SORN is to provide public notice of (1) the type of information being collected; (2) from whom or about whom it is being collected; (3) for what purpose/s it is being collected; and (4) with whom it may be shared and under what circumstances. See 5 U.S.C. 552a(e)(4). The ATS SORN describes the personal information ATS collects and maintains. The ATS PIA notes that, as a decision-support tool, the ATS system is employed to assist CBP officers in identifying travelers, cargo, and conveyances for further screening or examination. Due process rights that may flow from an enforcement action taken after an inspection or examination that was conducted as a result of initial ATS screening, are afforded in accordance with all applicable legal requirements.

Privacy Act Routine Use Comments

Comment: Routine Use A and B are so broad that they are meaningless.

Response: Routine Use A comprises standard language that has been used throughout the Federal Government to address the use of information contained in a law enforcement system. Routine Use A authorizes sharing with other law enforcement agencies in prosecuting or enforcing their respective statutes and regulations.

The revised ATS SORN does not include Routine Use B as originally set forth in the November 2, 2006 SORN.

Comment**:** Routine Use H duplicates and weakens the statutory condition of disclosure because it does not include the disclosure notification to the individual required by statute.

Response: CBP notes that this comment is actually in reference to Routine Use L not H. In the instance of a potential pandemic outbreak resulting from exposure to a communicable or quarantinable disease during travel and the possible subsequent dispersal throughout a region or the nation, CBP's first responsibility is to inform the proper health agencies and professionals of this risk to facilitate a rapid response to protect the public health. Routine Use L also eliminates potential duplicative reporting requirements to U.S. authorities responsible for protecting public health and combating pandemics. As such it reduces the economic burden on air carriers. It also promotes the privacy interest of travelers by minimizing the processing of their information by U.S. authorities.

Comment: Routine Use O is poorly written and seems to provide access to everyone but the individual who may be affected by a security breach. It should already be covered by subsection (b)(1) under the Privacy Act.

Response: Routine use O was added in response to recent information breaches at other agencies. This routine use was crafted by the Department of Justice in its work on the Identity Theft Task Force. (See "Combating Identity Theft: A Strategic Plan" at www.identitytheft.gov.) The commenter is correct that disclosures within the Department are covered by (b)(1); however, this routine use is not meant to cover this situation. Rather, following a breach DHS may need to share information with entities to facilitate notifying the affected individuals or conducting an investigation.

Comment: The ATS SORN fails to include any discussion of the safeguards in place concerning disclosure of ATS information, including the PNR held in ATS-P, to organizations outside of CBP.

Response: The updated ATS SORN that will publish in the Federal Register on August 6, 2007, describes safeguards provided for the information in ATS and in particular ATS-P. Additionally, the ATS PIA published on November 24, 2006 and republished on August 3, 2007, states that in any instance of sharing ATS information (including PNR) with an organization outside of DHS/CBP there is a Memorandum of Understanding, Letter of Exchange or other written arrangement that governs the exchange. CBP requires that the receiving agency have a relevant and legal purpose for receiving the information and properly protects the information against unauthorized disclosure before providing the receiving agency with access to the requested information. Additionally, as stated previously, access to the various ATS components is strictly regulated by DHS/CBP.

Privacy Act Exemption Comments

Comment: DHS's use of the TECS exemptions contravened the Privacy Act exemptions process.

Response: CBP was formed in part from a former component of the Department of the Treasury. This component last published the TECS SORN, as well as the regulation setting forth the basis for the various exemptions claimed by TECS and other systems of the former U.S. Customs Service. Because the TECS SORN covered ATS from ATS' development until DHS proposed a separate SORN for ATS , it was

appropriate for CBP to refer and cite to the former regulation as the basis for claiming exemptions pertaining to its new and current systems. Until such time as all of CBP's SORNs have been updated to reflect their inclusion within DHS, existing legacy SORNs from the former U.S. Customs Service and INS will continue to provide notice and coverage for existing CBP systems. Similarly, the exemption regulations for both the Department of Treasury and the Department of Justice will continue to satisfy the Privacy Act requirement for a regulation—indeed, this was the intent behind the enactment of the savings clause provisions in sections 1512 and 1517 of the Homeland Security Act of 2002.

Comment: Privacy Act (j)(2) exemption requirements are not met because the majority of the information collected/created by ATS is on law-abiding citizens who do not meet any of the three requirements of (j)(2), unless you assume that everyone crossing the border is the subject of criminal investigation or enforcement.

Response: Exemption (j)(2) permits CBP to assert an exemption for ATS because CBP is a law enforcement agency and the information in ATS is compiled to identify suspected and known criminal offenders or alleged criminal offenders. CBP is charged with screening all persons crossing U.S. borders to ensure compliance with U.S. laws. ATS exists, among other reasons, to assist DHS in identifying those persons who may be criminal offenders while not impeding the flow of legitimate travelers, cargo, and conveyances.

Comment: Privacy Act exemption (k)(2) requires that information be provided to affected individuals if they are denied any right, privilege, or benefit.

Response: The access provisions below include a clarifying amendment to the prior ATS SORN—namely, that an individual may gain access to his or her PNR data, upon request. CBP has long made this information available to U.S. and non-U.S. citizens and thus this represents only a clarification of the prior ATS SORN, not a change of policy.

Public Notice Comments

Comment: CBP has failed to give notice to all classes of individuals on whom information may be collected, including non-travelers who have provided information during the reservation process that is later transmitted as part of the traveler's PNR.

Response: Publication in the Federal Register constitutes official notice to the world. In the prior ATS SORN, CBP made clear that it was collecting information in ATS-P that pertains to persons crossing the U.S. border. More specifically, that SORN set forth the information elements generally described as PNR, including "Travel agent." This is one information element that does not pertain to the traveler but is nevertheless included in the PNR submitted to CBP. CBP is prepared to work with interested parties to improve public awareness about existing CBP policies and the public's rights under this SORN and other applicable DHS policies. To increase transparency, this updated SORN adds the following under category of individuals: "Persons who serve as booking agents, brokers, or other persons who provide information on behalf of persons seeking to enter or exit the United States."

Comment: The PIA fails to explain how ATS operates with respect to passengers exiting the United States.

Response: CBP has posted an amended PIA on its web site which addresses the changes to the prior ATS SORN described in this notice. These amendments include clarification of the discussion about ATS-P and persons exiting the United States.

Comment: The timing of ATS SORN is too close to implementation.

Response: This comment misunderstands the implementation of ATS. As noted earlier, ATS-P has been operational since approximately 1999 and has been covered by the TECS SORN. The purpose of the ATS SORN was to separate ATS from the TECS SORN to provide more transparency into ATS, as well as ensure greater protection for the information stored in that system by maintaining it apart from information contained in other enforcement databases.

Comment: What safeguards are there to ensure that PNR is not used improperly?

Response: CBP recognizes the potential for misuse of PNR data and any information that it collects. CBP, therefore, has implemented several internal controls to mitigate this threat to the integrity of its systems. Access to CBP's systems is governed by a strict policy that implements rights and responsibilities to information—this means that employees only have access to information that falls within their need to know. CBP requires that all employees attend regular privacy awareness training to receive automated systems access and requires that employees periodically re-attend such training to continue access. CBP also identifies misuse of information in information systems as a specific violation within its Table of Offenses applicable to all employees. Employees may be dismissed from CBP for mishandling or misusing information maintained in CBP's systems and may be subject to criminal or civil penalties.

System is Ineffective or Unfairly Discriminates Comments

Comment: ATS' data mining is an ineffective and inefficient use of resources.

Response: As an initial matter, ATS-P is not a data-mining activity, as defined by Congress. Conference Report on HR 5441, DHS Appropriations Act, House Report No. 109-699, Sept. 28, 2006, H7784, at H7815 uses the following definition for "data mining": "a query or search or other analysis of 1 or more electronic databases, whereas – (A) at least 1 of the databases was obtained from or remains under the control of a non-Federal entity, or the information was acquired initially by another department or agency of the Federal Government for purposes other than intelligence or law enforcement; (B) a department or agency of the Federal Government or a non-Federal entity acting on behalf of the Federal Government is conducting the query or search or other analysis to find a predictive pattern indicating terrorist or criminal activity; and (C) the search does not use a specific individual's personal identifiers to acquire information concerning that individual." ATS-P's risk assessments, by contrast, are based on predicated and contextual law enforcement and intelligence data.

Furthermore, ATS actually increases the efficiency of border officers by reducing the number of system queries they must conduct to perform their jobs. Without ATS-P, for example, border officers would be forced to perform separate queries in each different TECS modules to obtain the same data. In addition, although the decision to subject a traveler, conveyance, or shipment to additional scrutiny or to initiate an enforcement action remains with the appropriate DHS official, the various ATS components assist in

narrowing the scope of a likely examination by applying collective and current intelligence and past case experience

General Legal or Constitutional Comments

Comment: This type of targeting is banned by Congress.

Response: CBP's collection of PNR information is expressly authorized by the Congress in the Aviation and Transportation Security Act of 2001 (ATSA). Congress has not imposed any independent restriction on CBP using ATS-P for passenger screening. To the contrary, in fiscal years 2005 and 2006, Congress appropriated $37 million and $28 million respectively for ATS's Passenger Screening Program.

Section 514 of the 2007 Homeland Security Appropriations Act, Pub. L. 109-295, which restricts the use of appropriated funds for the "Secure Flight program or any other follow-on or successor passenger prescreening program," does not restrict CBP's use of ATS-P. Section 514 is concerned only with aviation security generally and the Secure Flight program administered by the Transportation Security Administration in particular. Congress did not intend section 514 to pertain to ATS, a program that has been funded by Congress since the late 1990's and has an entirely different mission from Secure Flight: Secure Flight is intended to screen domestic passengers attempting to board airplanes; ATS-P relates to individuals seeking admission to the U.S. at ports of entry. Furthermore, because ATS (and more specifically, ATS-P) preceded the above program, it cannot be considered its "follow-on or successor."

Comment: PNR contains domestic flight data, the use of which is impermissible.

Response: PNR collected by CBP pursuant to its authority under 49 U.S.C. 44909 and screened using ATS-P only contains domestic flight data where there is a domestic leg to an international transit. CBP is authorized to collect PNR information pertaining to all persons crossing the U.S. border. The ATSA defines international travel as beginning with any domestic flight that connects directly to an international flight as part of the same travel itinerary.

Comment: ATS, including ATS-P, is unconstitutional. ATS violates the Fourth Amendment and the Second Amendment of the U.S Constitution (i.e., the right to bear arms).

Response: As the Supreme Court has stated, "[i]t is axiomatic that the United States, as sovereign, has the inherent authority to protect, and a paramount interest in protecting, its territorial integrity." *United States v. Flores-Montano*, 541 U.S. 149, 153 (2004). Indeed, "the Government's interest in preventing the entry of unwanted persons and effects is at its zenith at the international border." *Id.* at 152. For this reason, the Supreme Court has held that stops and examinations are reasonable in the absence of a warrant or probable cause when they are conducted at the U.S. border, *see Carroll v. United States*, 267 U.S. 132, 153–54 (1925), and the "functional equivalent of the border," such as international airports, *see United States v. Irving*, 432 F.3d 401, 414 (2d Cir. 2005).

Under the border search exception, routine stops and examinations conducted at the border are reasonable for Fourth Amendment purposes "simply by virtue of the fact that they occur at the border," and may be conducted without any individualized suspicion. *United States v. Ramsey*, 431 U.S. 606, 616 (1977). The Government

conducts border stops and examinations—whether manually or with the assistance of automated systems like ATS—"pursuant to the longstanding right of the sovereign to protect itself by stopping and examining persons and property crossing into this country.'" *Flores-Montano*, 541 U.S. at 152–53 (quoting *Ramsey*, 431 U.S. at 616). CBP's broad authority to conduct activities relating to the entry or exit of persons or things into or out of the United States is codified at title 19 of the U.S.C. § 482, 1461, 1496, 1499, and 1581-83, and title 8, U.S.C. § 1357. ATS is a decision-support tool used by CBP officers to execute this lawful border enforcement authority and thus does not violate any right to privacy.

Additionally, individuals are permitted to travel with certain types of firearms so long as they are properly secured and other procedures are followed. CBP's inspection of persons, conveyances, and cargo attempting to cross the border—as the result of ATS or otherwise—does not affect this or in any way violate the Second Amendment.

Comment: ATS improperly discriminates against those crossing the border, including based on race and religion.

Response: Consistent with the border enforcement mission described above, CBP is authorized to screen all persons and goods crossing the border. ATS-P's automated screening of travelers utilizes TSDB, information on individuals with outstanding wants or warrants, or information from other government agencies regarding high risk parties and paradigms based on law enforcement data, intelligence, and past case experience; it does not unconstitutionally discriminate based on religion, nationality, ethnicity, race, or gender. CBP policy prohibits improper discrimination based on race or religion and violators are subject to the penalties described in CBP's Table of Offenses.

Comment: CBP's use of ATS requires legislative and judicial oversight. Moreover, ATS denies individuals a right to judicial review.

Response: DHS already receives significant and constructive oversight by Congress, the Inspector General and the DHS Privacy Office with respect to many of its programs, including ATS. Individuals are entitled to judicial review of most enforcement actions taken by CBP as a result of ATS.

Comment: The sharing of individuals' risk scores with the private sector alters the fundamental relationship between the state and individuals: the private sector is deputized to act on state or local warrants.

Response: Unlike the ATS components relating to cargo, ATS-P does not assign a "risk score" to travelers. DHS will only share information in ATS in accordance with the Privacy Act (including the routine uses noted in the SORN), or as otherwise required by law. As a matter of practice, ATS-P risk assessments are rarely shared outside DHS and, to the extent they are shared, they are shared only with other government authorities who have a need-to-know for purpose of carrying out their official responsibilities.

Moreover, ATS does not change the relationship between the state and the individual. At no time are airline representatives or others in the private sector deputized to enforce state or local warrants. This authority remains within the purview of the government.

Comment: ATS contravenes the Airline Deregulation Act of 1978 and International Commitment on Civil and Political Rights.

Response: The Airline Deregulations Act resulted in the reduction of government regulation over airline issues such as fares, routes, and schedules. The International

Covenant on Civil and Political Rights, a United Nations treaty which entered into force in 1976, concerns the protection of human rights. Neither of these purports to restrict or otherwise affect CBP's use of ATS to carry out CBP's mission to protect the United States against terrorism and enforce U.S. laws.

Recommended Actions Comments

Comment: DHS should create an Advisory Committee for Privacy.

Response: Pursuant to the Federal Advisory Committee Act, DHS already has established the Data Privacy and Integrity Advisory Committee to advise the Secretary and the Chief Privacy Officer of DHS on programmatic, policy, operational, administrative, and technological issues within DHS that affect individual privacy, data integrity and interoperability, and other privacy related issues.